UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,470	01/05/2001	Steven Branigan		4994

27997   7590   11/27/2007
PRIEST & GOLDSTEIN PLLC
5015 SOUTHPARK DRIVE
SUITE 230
DURHAM, NC 27713-7736

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

MAILED

Application Number: 09/755,470
Filing Date: January 05, 2001
Appellant(s): BRANIGAN ET AL.

NOV 27 2007

Technology Center 2100

Peter Priest
Reg. No. 30,210
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12 October 2007 appealing from the Office action

mailed 13 April 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings

which will directly affect or be directly affected by or have a bearing on the Board's decision in

the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in

the brief is correct. The amendment filed 12 October 2007 to correct a typographical error in

claim 7 has been accepted and entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct. The

copy in the Appeal Brief does not contain the typographical correction to claim 7, entered in

amendment filed 12 October 2007.

(8) Evidence Relied Upon

<u>Massarani U.S. Patent No. 6,393,484</u> – "An object of this invention is a system and method
which makes it impossible or very difficult for unauthorized devices and users to obtain IP
network services on shared-medium public and semi-public networks ... This is accomplished in
a system comprising OSI layer work equipment (routers and/or switches) which work in
conjunction with a Dynamic Host Control Protocol (DHCP) server and Address Resolution
Protocol (ARP)
(col. 3, lines 6-30).
NOTE: The DHCP server or authentication server authenticates the mobile device and provides
an IP address.

<u>Lewis U.S. Patent No. 6,526,506</u> – "The present invention relates generally to wireless networks,
and more particularly to an encryption scheme and access point for providing two or more levels
of encryption to prevent unauthorized access to the network" (col. 1, lines 6-10).
NOTE: This invention teaches encryption and encryption key exchange between mobile
devices.

<u>Bhagwat et al. U.S. Patent No. 6,651,105</u> – "In another embodiment, the present invention
establishes a persistent PPP connection between a mobile device and a PPP server. Instead of
running a PPP server on each wireless access point, the PPP function is aggregated into a server
located in the network. The access point acts like a PPP proxy, bridging the wireless and the
wired medium. On the wireless side the access point emulates an RS-232 lines, while on the
wireline side the access point emulates a byte stream tunnel to the PPP server. When a portable
device moves, it notifies its PPP peer using a new PPP option to switch the byte stream tunnel to
another access point. Since the portable device carries its PPP state with it, it always remains
connected to the same PPP server as before (albeit over a different emulated wire). No change in
IP address is required and, consequently, none of the active connections are disrupted" (col. 3,
lines 47-63).
NOTE: This invention teaches the ability for mobile devices to roam without having to re-
establish connection with server to obtain authorization to utilize network.

<u>Redlich U.S. Patent No. 6,651,306</u>– "It is a further object of the invention to achieve instant IP
connectivity in a manner which prevents malicious attacks to the hosting network by the guest
station. An additional object of the invention is to achieve the foregoing connectivity in a

manner which permits the guest station, if desired, to provide for security against malicious
intrusion or attacks from the foreign network" (col. 14, lines 29-37).
NOTE: This invention teaches guest wireless devices authorized to utilize foreign networks
without compromising security. This is accomplished by an intelligent router that utilizes a 128-
bit encryption key.

Schuster et al. U.S. Patent No. 6,857,072 – Teaches mobile wireless devices utilizing public key
encryption.

NOTE: All of the above references are directed to (mobile) wireless communications and

devices

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1 and 7, are rejected under 35 U.S.C. 103(a) as being unpatentable over

Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506

(hereinafter '506).

Regarding claim 1,

As per the first limitation, **"A wired network for providing secure, authenticated**

access to wireless network clients, comprising: a server connected to a wireless network

access point, and having access to the wired network, the server being operative to perform

authentication for a wireless client" is taught in '484 col. 4, lines 31-66.

As per the second limitation, **"establishing a connection to the server through the**

wireless network access point, the server performing authentication by examining

authentication information transmitted from the client to the server" is disclosed in '484

col. 5, lines 7-25.

As per the third limitation, **"and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client,"** is taught in '484 col. 4, lines 31-41 and also see col. 6, lines 23-53.

As per the fourth limitation, **"the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key to the client to be used for encrypted communication with the wired network and valid for the connection session upon authentication of the client"** is disclosed in '506 col. 11, line 64 through col. 12, line 26 "the key distribution server 76 responds to the encrypted request packet with a response packet containing the ENCRYPT key in its data field as is discussed below in relation to FIG. 8. The processor 142 passes the response packet through the encryption engine 146 in order to encrypt the response packet using the MASTER key. The response packet is addressed to the mobile terminal 66 requesting the ENCRYPT key, and is transmitted out onto the system backbone 52. The access point 54 with which the mobile terminal 66 is registered will detect and receive the response packet by detecting the network address of the mobile terminal in the destination address of the non-encrypted header field. The access points 54, in the preferred embodiment, are also configured to detect from the header field when a packet originates from the key distribution server 76 (as noted from the source address of the header field). In the event a packet originates from the key distribution server 76 as in the case of an ENCRYPT key response packet, the access points 54 are configured not to encrypt the packet via the ENCRYPT key and the encryption engine 118. Rather, the packet is simply

forwarded to the destination mobile terminal 66 without encryption via the ENCRYPT key as

discussed below in relation to FIG. 9. However, this will not jeopardize system security as will

be appreciated since the response packet containing the ENCRYPT key already has been

encrypted using the MASTER key by the key distribution server 76. Thus, the mobile terminal

66 may still be informed of the ENCRYPT key via the wireless link without jeopardizing system

security". Note as explained the response to the client (i.e. mobile terminal) is encrypted with

the client's MASTER key, this is the encrypted communications exchanged with the AP then

forwarded to the client, that contains the cryptographic key valid for the session (the ENCRYPT

key).

As per the fifth limitation, **"and a user database accessible to the server for use in**

validating wireless clients" is shown in '484 col. 5, lines 8-19.

Claim 7 is an independent claim containing limitations similar to claim 1.

Claims 2-5, 8-13, are rejected under 35 U.S.C. 103(a) as being unpatentable over

Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506

(hereinafter '506) in further view of Bhagwat et al. US Patent No. 6,651,105 (hereinafter '105).

Regarding claim 10,

As per the first limitation, **"A method of secure communication between wireless**

network clients and a wired network, comprising the steps of: establishing a connection

between a wireless network access point and a security base (SB) server connected to the

wired network; establishing a connection between the SB server and a wireless network

client communicating with the SB server through the wireless network access point" is

taught in '484 col. 4, lines 31-66.

As per the second limitation, **"exchanging encryption keys between the SB server and the wireless network client"** is taught in '506 col. 11, line 64 through col. 12, line 26, the server provides the ENCRYPT key to the mobile terminal, this key is used in the wireless communication session in.

As per the third limitation, **"transmitting authentication information from the wireless network client to the SB server through the wireless network access point; performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network if authentication fails, rejecting connection to the wired network and if authentication passes, accepting connection to the wired network, providing a temporary wired network address"** is taught in '484 col. 6, lines 23-53;

As per the fourth limitation, **"and a unique session encryption key to the wireless network client for encrypted communication with the wired network and valid for the connection session"** is taught in '506 col. 11, line 64 through col. 12, line 26, the ENCRYPT key provided is used for encrypted communication with the designated Access point in;

As per the fifth limitation, **"and providing access to wired network resources in response to requests by the wireless network client"** is taught in '105 col. 3, lines 41-48, note additional resources is an obvious variation of peers.

Regarding claim 11,

As per the first limitation, **"and wherein the step of accepting the connection is accompanied by a step of logging the acceptance"** is taught in '484 col. 5, lines 17-19.

As per the second limitation, **"wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection"** is shown in '484 col. 6, lines 11-23.

Regarding claim 12,

As per the first limitation, **"wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address" "** is disclosed in '484 col. 3, lines 47-50.

Regarding claim 2,

As per the first limitation, **"also including a network hub providing connections between the server"** is taught in '484 FIG. 1 the edge router switch inherently is the network hub.

As per the second limitation, **"and additional resources on the wired network"** however '105 teaches in col. 3, lines 41-48, note additional resources is an obvious variation of peers.

Regarding claim 3,

As per the first limitation, **"also including a router providing connections between the server"** is taught in '484 col. 4, lines 54-67.

As per the second limitation, **"and additional resources on the wired network"** however '105 teaches in col. 3, lines 41-48, note additional resources is an obvious variation of peers.

As per the third limitation, **"as well as a connection to an additional wired network"** is shown in '484 col. 5, lines 55-65

Regarding claim 4,

As per the first limitation, **"wherein the server is operative to provide addresses to clients through dynamic host control protocol"** is disclosed in '484 col. 3, lines 47-50.

Regarding claim 5,

As per the first limitation, **"wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol"** however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54.

Regarding claim 8,

As per the first limitation, **"wherein the access point communicates with the server using point to point tunneling protocol"** however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54.

Regarding claim 9,

As per the first limitation, **"including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and- the additional network access points being operative to establish connections with the server through the network hub"** is shown in '484 col. 4, lines 54-65.

Regarding claim 13,

As per the first limitation, **"wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol"** however '105 teaches PPP is used for communications between the server and the wireless client in col. 4, lines 36-54.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506) in further view of Bhagwat et al. US Patent No. 6,651,105 (hereinafter '105) in further view of Redlich US Patent No. 6,591,306 (hereinafter '306).

Regarding claim 6,

As per the first limitation, **"wherein the server employs 128-bit crypto-processing to communicate with the wireless network client"** is taught in '306 col. 25, lines 43-67, a 128 bit encryption key can be utilized in communication.

Claim 14 and 15, are rejected under 35 U.S.C. 103(a) as being unpatentable over Massarani US Patent No. 6,393,484 (hereinafter '484) in view of Lewis US Patent No. 6,526,506 (hereinafter '506) in further view of Bhagwat et al. US Patent No. 6,651,105 (hereinafter '105) in further view of Schuster et al. U.S. Patent No. 6,857,072 (hereinafter '072).

Regarding claim 14,

As per the first limitation, **"wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server"** is taught in '484 col. 6, lines 23-53;

"and wherein the authentication information is encrypted" is taught in '105 col. 4, lines 36-54 and also col. 2, lines 20-24, 'Point-to-point protocol (PPP) is used for communication for wireless devices via access points. This communication can be encrypted if required'

As per the second limitation, **"using public key cryptography"** is taught in '072 col. 6, lines 44-64, the use of a public key to encrypt data transmitted over a network.

Regarding claim 15,

As per the first limitation, **"wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key using public key cryptography"** is taught in '072 col. 6, lines 44-64, the use of a public key to encrypt data transmitted over a network.

(10) Response to Argument

Regarding Applicant's first argument, on page 7 which is later reiterated in the

Applicant's closing arguments in pages 13-17,

> "The final rejection under 35 U.S.C. 103 did not follow M.P.E.P 706.02(j) which states:
>
> After indicating that the rejection under 35 U.S.C. 105, the Examiner should set
> forth…the difference or differences in the claim over the applied reference…the
> proposed modification of the applied reference(s) necessary to arrive at the claimed
> subject matter, and…an explanation why one of ordinary skill in the art at the time the
> invention was made would have been motivated to make the proposed modification …

The art rejections are not supported by relied upon art. All of the rejections are based on

Massarani in combination with one, two, or three other items. Such analysis should consider

whether the modifications are actually suggested by the references rather than assuming they are

obvious … This approach constitutes impermissible hindsight and must be avoided … The

Examiner's rejection suggest that the Examiner did not consider and appreciate the claim as a

whole".

The Examiner's disagrees with argument for multiple reasons, first the 'Evidence relied upon'

described in section 8 show how all the references are directed to (mobile) wireless

communications and devices, that is why it is obvious to combine. The KSR ruling indicates it is

permissible to combine prior art references from the same endeavor. Second as shown by the

long case history with three Non-Final Actions, three Final Actions along with four submissions

of Affidavits in:

2 May 2005, 30 November 2005, 6 February 2006, and 17 July 2006 in order to overcome the

various references applied in the rejections that the combination is not novel. Since many

wireless communication devices applications contain similar features. <u>Third</u> the combination is

also similar to 802.11 standards issued for wireless communications.

Regarding Applicant's second argument, beginning on page 7, "Claims 1 and 7 ... As

such Massarani is a very poor reference for purposes of any obviousness analysis, as-if anything-

it teaches away from the presently claim invention".

The Examiner disagrees with the argument, Massarani teaches in the prior art the problems are

that they rely on complex and inflexible methods. Massarani does not teach away from

encryption, rather Massarani teaches away from requiring a mobile device to maintain the same

IP address and a complex key management system.

Regarding Applicant's third argument, beginning on page 8, "The Official Action

correctly admits at pages 3 and 4 that Massarani fails to teach both "the server being further

operative to encrypt communications with the wireless network access point" and "the server

being further operative to provide a cryptographic key valid to the client for encrypted

communication and valid for connection session upon authentication of client ... Lewis does not

provide a basis for modifying Massarani to meet the present claims. First, however, Massarani

does not meet other elements of both claims 1 and 7, and the analysis of the Official Action at

page 3, paragraph 6 (claim 1) and pages 6 and 7 (claim 7) are fundamentally flawed and

incorrect ... By contrast, in the present claims, the SB server controls access to the wired

network ... Apparently, the Official Action relies upon DHCP server 30 or optional

authentication server 36 of Massarani as performing this claimed operation and function.

However, these servers are connected to the access ports through layers of edge routers/switches

.. and the edge routers/switch 20 so that the boundary of the network 14 is not protected by these

servers in the same way SB server 102 protects network 100 for example".

The Examiner disagrees with argument all that is claim is that the server authenticates the client

before access is granted, Massarani performs the same function. In addition, the Examiner

disagrees with the arguments that analyze Massarani drawing against applicants specification

and drawings. The claims are interpreted in light of the specification however limitations from

the specification are not placed into the claims.

Regarding Applicant's fourth argument, beginning on page 10, "Claim 1 also recites that

the server provides "the client with a wired network address valid for the connection session" ...

However, this relied upon text clearly does not literally or inherently meet the quoted language

from claim 1".

The Examiner disagrees with the argument and notes the supplied IP address from the DHCP is

interpreted equivalent to the "a wired network address valid for the connection session". As

shown a device authentication process is initiated if the device fails authentication the DHCP

server will not provide allow IP communications. ·

Regarding Applicant's fifth argument, beginning on page 11, "Returning to Lewis, Lewis

like Massarani shows an arrangement in which access points serve as entrance points directly to

the wired network ... Thus, Lewis provides no basis for modifying Massarani in a manner so as

to meet the present claims, and effectively teaches away from the present claims".

The Examiner disagrees with argument as already shown Massarani teaches the server connected

to the network, both references are directed to wireless communication and devices therefore the

combination is relevant.

Regarding Applicant's sixth argument, on page 12, "Claim 7 was rejected on similar

basis claim 1, ant it is allowable on the basis argued above. However, it is further noted that

claim 7 focuses on details of the "wireless network access point" and specifically recites

"connection with a server operations as a portable between the wireless network and a wired

network". It does not appear that any server of Massarani or Lewis operates in such a manner".

The Examiner disagrees with arguments as shown above claim 1 is rejected with the combination

of Massarani and Lewis. In addition Massarani teaches the server authenticating the wireless

client before access is allowed. The server in Lewis encrypts communications with the client,

therefore a portal is established.

Regarding Applicant's seventh argument, beginning on page 12, "Claims 2-5 and 8-12

stand rejected based on Massarani in view of Lewis in further view of Bhgwhat ... Claim 10

further recites "providing access to wired network resources in response to request by the

wireless-client" which the Official Action admits "is not explicitly taught in Massarani and

Lewis relying on Bhagwhat at col. 3, lines 41-48. This portion of Bhagwhat addresses

preserving an already established PPP connection during hang-offs when a mobile moves to a

new access point. This disclosure of Bhagwhat does not meet the above recited language of

claim 10 ... nothing, in the cited portion of Bhagwhat suggests anything beyond a handoff in

which the status quo is simply maintained".

The Examiner disagrees with argument for multiple reasons. As previously stated with respect

to arguments present toward the rejection of claim 1 and 7, Massarani and Lewis teach all the

limitations. In addition the portion of claim 10 that is rejected by Bhagwhat is in bold text

below:

"and a unique session encryption key to the wireless network client for encrypted

communication with the wired network and valid for the connection session"

Bhagwhat is used to establish that it is taught in the prior art that 'unique session

encryption keys' are provided to wireless devices. The 'session key' is considered equivalent to

a key that is provided to a wireless device in order to communicate with a designated access

point.

Regarding Applicant's eighth argument, on page 13, "With regard to claim 2, the Official

Action suggest Massarani's edge router switch meets the claims "network hub",; however, the

pertinent portion of claim 2 reads in full "a network hub providing connections between the

server and additional resources of the wired network". The edge router/switches 20^1 and 22^N of

Massarani do not meet the terms of claim 2. As seen in Fig. 1 of the present application ... This

noted difference is significant because as noted above a server, such as SB server 102 of Fig. 1 of claim 1 effectively guards the door to the network 100. The claimed arrangement of the network hub of claim 2 server to further emphasize this distinction and further distinguishes the very different structure addressed by Massarani".

The Examiner disagrees with the argument for numerous reasons. First although the claims are interpreted in light of the specification and drawings, limitations from the specification are not placed into the claims. Second the Applicant is addressing the references individually when it was the combination that was used to reject claim 2.

Regarding Applicant's ninth argument, on page 13, "As to the remaining dependent claims, the additionally relied upon items do not cure the deficiencies of Massarani and Lewis addressed above"

The Examiner disagrees as explained above the combination is obvious because both Lewis and Massarani are directed to wireless devices and communications. In addition all the features of the claims are taught.
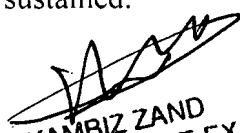
(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

/Ellen Tran/
Patent Examiner
Technology Center 2134
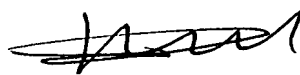
Conferees:

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kim Vu

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kambiz Zand